ИНФОРМАЦИОННОЕ СООБЩЕНИЕ
о разработке методического документа ФСТЭК России «Методика определения угроз безопасности информации в информационных системах»

от 9 апреля 2020 г. № 240/22/1534

В соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, ФСТЭК России разработан проект методического документа «Методика моделирования угроз безопасности информации».

Документ определяет порядок и содержание работ по моделированию угроз безопасности информации, включая персональные данные, в информационных (автоматизированных) системах, автоматизированных системах управления, информационно-телекоммуникационных сетях, в том числе отнесенных к объектам критической информационной инфраструктуры Российской Федерации, в информационно-телекоммуникационных инфраструктурах центров обработки данных и облачных инфраструктурах, защита информации в которых или безопасность которых обеспечивается в соответствии с требованиями по защите информации (обеспечению безопасности), утвержденными ФСТЭК России в пределах своей компетенции.

Методический документ должен применяться совместно с банком данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru).

В целях реализации положений методического документа планируется модернизация раздела «Угрозы» банка данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru).

Проект указанного документа размещен на официальном сайте ФСТЭК России www.fstec.ru в разделе «Техническая защита информации/Документы/Проекты».

ФСТЭК России предлагает специалистам в области информационной безопасности заинтересованных органов государственной власти, субъектов критической информационной инфраструктуры и организаций рассмотреть проект методического документа и направить предложения по указанному документу в соответствии с прилагаемой формой на адрес электронной почты otd22@fstec.ru.

Предложения и замечания по проекту методического документа принимаются до 30 апреля 2020 г.

Заместитель директора ФСТЭК России В.Лютиков

Форма направления в ФСТЭК России замечаний
и предложений по результатам рассмотрения проекта методического документа ФСТЭК России «Методика определения угроз безопасности информации в информационных системах» (далее – проект Методики)

№ п/п	**№ пункта проекта Методики**	**Содержание замечания (предложения)**	**Предлагаемая редакция пункта проекта Методики**
1			
…			
n			

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

Утвержден ФСТЭК России

« » _____ 2020 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА
МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

ПРОЕКТ

2020

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Методика моделирования угроз безопасности информации (далее – Методика) разработана в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утверждённого Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

1.2. Методика определяет порядок и содержание работ по моделированию угроз безопасности информации, включая персональные данные, в информационных (автоматизированных) системах, автоматизированных системах управления, информационно-телекоммуникационных сетях, в том числе отнесенных к объектам критической информационной инфраструктуры Российской Федерации, в информационно-телекоммуникационных инфраструктурах центров обработки данных и облачных инфраструктурах, защита информации в которых или безопасность которых обеспечивается в соответствии с требованиями по защите информации (обеспечению безопасности), утвержденными ФСТЭК России в пределах своей компетенции (далее – системы и сети).

1.3. Методика ориентирована на выявление и оценку антропогенных угроз безопасности информации, возникновение которых обусловлено действиями нарушителей. Часть приведенных в Методике подходов может применяться для оценки техногенных угроз в случае, если они позволяют достичь целей такой оценки.

1.4. В документе не рассматриваются методические подходы по моделированию угроз безопасности информации, связанных с нарушением безопасности шифровальных (криптографических) средств защиты информации, а также угроз, связанных с техническими каналами утечки информации.

1.5. Выявление угроз, связанных со стихийными бедствиями и природными явлениями, осуществляется в соответствии с требованиями и правилами, установленными уполномоченными федеральными органами исполнительной власти, национальными стандартами, и не входит в область действия настоящей Методики.

1.6. На основе настоящей Методики могут разрабатываться отраслевые (ведомственные, корпоративные) методики моделирования угроз безопасности информации, которые учитывают особенности функционирования систем и сетей в соответствующей области деятельности. Разрабатываемые отраслевые

(ведомственные, корпоративные) методики моделирования угроз безопасности информации не должны противоречить положениям настоящей Методики.

1.7. В Методике используются термины и определения, приведенные в приложении № 1 к настоящей Методике, а также термины и определения, установленные законодательством Российской Федерации и национальными стандартами в области защиты информации и обеспечения информационной безопасности.

1.8. Методика применяется совместно с банком данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), а также базовыми и типовыми моделями угроз безопасности информации, разрабатываемыми ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

1.9. В связи с утверждением настоящего методического документа не применяется для определения угроз безопасности информации Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ФСТЭК России, 2008 г.) и Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (ФСТЭК России, 2007 г.).

2. ПОРЯДОК МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И РАЗРАБОТКИ МОДЕЛЕЙ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

2.1. Целью моделирования угроз безопасности информации является выявление совокупности условий и факторов, которые приводят или могут привести к нарушению безопасности обрабатываемой в системах и сетях информации (нарушению конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации и (или) средств её обработки), а также к нарушению или прекращению функционирования систем и сетей.

В качестве угроз безопасности информации, подлежащих определению при моделировании угроз безопасности информации, рассматриваются неправомерные действия и (или) воздействия на информационные ресурсы или компоненты систем или сетей, в результате которых возможно нарушение безопасности информации и (или) нарушение или прекращение функционирования систем и сетей, повлекшее наступление негативных последствий.

Пример 1: *1) получение несанкционированного доступа к персональным данным, содержащимся в базе данных, в результате которого возможно нарушение их конфиденциальности; 2) изменение (модификация) уставок устройства, приводящее к прекращению функционирования релейной защиты и автоматики в аварийной ситуации; 3) несанкционированный доступ к программируемому логическому контроллеру, в результате которого возможно включение выключателя подачи электроэнергии цифровой электроподстанции; 3) отказ в обслуживании маршрутизатора информационно-телекоммуникационной сети, в результате которого возможно прекращение передачи данных*

2.2. В результате моделирования угроз безопасности информации должен быть сформирован перечень угроз безопасности информации, реализуемых для рассматриваемой архитектуры и условий функционирования систем и сетей.

2.3. Процесс моделирования угроз безопасности информации включает (рисунок 1):

1) определение возможных негативных последствий от реализации угроз безопасности информации;

2) определение условий для реализации угроз безопасности информации;

3) определение источников угроз безопасности информации и оценку возможностей нарушителей;

4) определение сценариев реализации угроз безопасности информации;

5) оценку уровня опасности угроз безопасности информации.

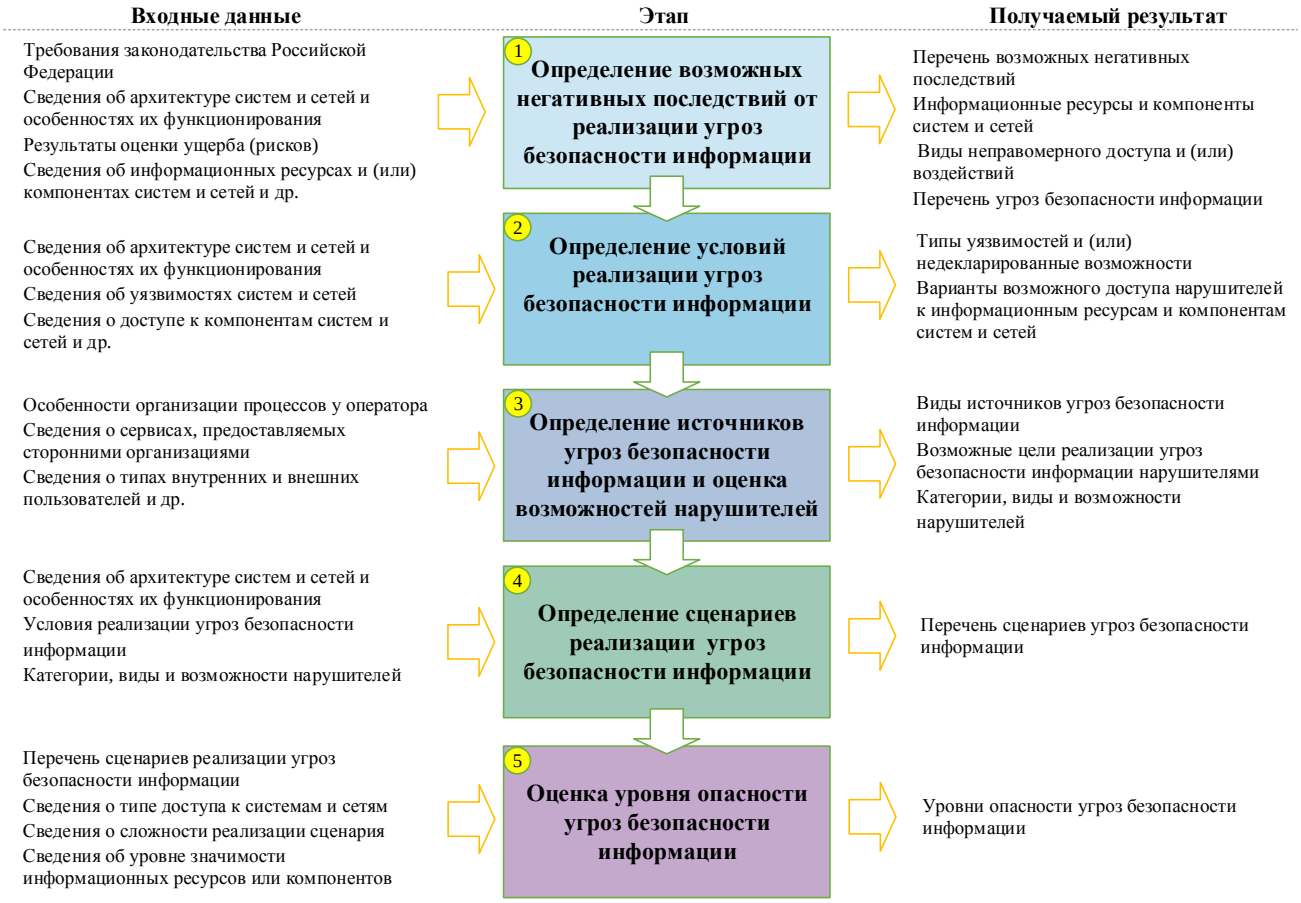

Рисунок 1 – Процесс моделирования угроз безопасности информации

2.4. При моделировании угроз безопасности информации определяется граница процесса моделирования, в которую включаются информационные ресурсы и компоненты систем и сетей, обрабатывающие, хранящие информацию и (или) обеспечивающие реализацию основных (критических) процессов (бизнес-процессов) обладателя информации и оператора, интерфейсы их взаимодействия с пользователями, со смежными (взаимодействующими) системами и сетями, а также инженерные системы (системы электроснабжения, вентиляции, охлаждения, кондиционирования, охраны, системы охраны), средства, каналы и услуги связи, другие услуги и сервисы, предоставляемые сторонними организациями, от которых зависит функционирование систем и сетей (далее – обеспечивающие системы).

К основным (критическим) процессам (бизнес-процессам) относятся управленческие, технологические, производственные, финансово-экономические и другие процессы (бизнес-процессы), выполняемые обладателем информации и оператором в рамках реализации функций (полномочий) или осуществления основных видов деятельности.

Процессом моделирования угроз безопасности информации должны быть охвачены все информационные ресурсы и компоненты систем и сетей, составляющих информационную инфраструктуру обладателя информации и (или) оператора, неправомерный доступ к которым или воздействие на которые может привести к негативным последствиям.

2.5. Моделирование угроз безопасности информации должно носить систематический характер и осуществляться как на этапе создания систем и сетей и формирования требований по их защите, так и в ходе их эксплуатации. Систематический подход к моделированию угроз безопасности информации позволяет поддерживать адекватную и эффективную систему защиты в условиях изменения угроз безопасности информации и информационных ресурсов. Учет изменений угроз безопасности информации способствует своевременной выработке адекватных мер защиты информации (обеспечения безопасности).

2.6. На этапе создания систем и сетей моделирование угроз безопасности информации проводится на основе их предполагаемой архитектуры и должно быть направлено на обоснованный выбор организационных мер, функциональных возможностей и настроек средств защиты информации. На этапе эксплуатации систем и сетей моделирование угроз безопасности информации проводится для реальной архитектуры систем и сетей и условий их функционирования и должно быть направлено на выявление изменений угроз безопасности информации и оценку эффективности применяемых мер и средств защиты информации.

2.7. Моделирование угроз безопасности информации должно проводиться с учетом применяемых в системах и сетях в соответствии с требованиями нормативных правовых актов Российской Федерации и (или) технических заданий средств защиты информации. Однако при этом необходимо учитывать возможность наличия в организации работ и применяемых средствах защиты информации уязвимостей, которые могут использоваться для реализации угроз безопасности информации.

2.8. Моделирование угроз безопасности информации проводится подразделением по защите информации обладателя информации или оператора,

или отдельными специалистами, назначенными ответственными за защиту информации (обеспечение безопасности), с участием в том числе подразделений и специалистов, ответственных за эксплуатацию систем и сетей (ИТ-специалистов), а также основных подразделений обладателя информации и оператора.

К моделированию угроз безопасности информации могут привлекаться организации, имеющие лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации. В этом случае обладателем информации и (или) оператором предоставляется вся информация о системах и сетях, условиях их функционирования, необходимая для моделирования угроз безопасности информации в соответствии с настоящей Методикой.

2.9. Для проведения оценок, в основе которых лежат экспертные методы, могут создаваться экспертные группы. В частности, экспертный метод может применяться для оценки возможных последствий от реализации угроз безопасности информации, определения возможных целей реализации угроз безопасности информации, сценариев реализации угроз безопасности информации. Рекомендации по формированию экспертной группы и проведению экспертной оценки приведены в приложении № 2 к настоящей Методике.

2.10. В случае моделирования угроз безопасности информации для систем и сетей, функционирующих на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, угрозы безопасности информации определяются как для самих систем и сетей, так и для информационно-телекоммуникационной инфраструктуры, на которой они функционируют. Пример границы процесса моделирования угроз безопасности информации систем и сетей, функционирующих на базе информационно-телекоммуникационной инфраструктуры центра обработки данных, приведен на рисунке 2.

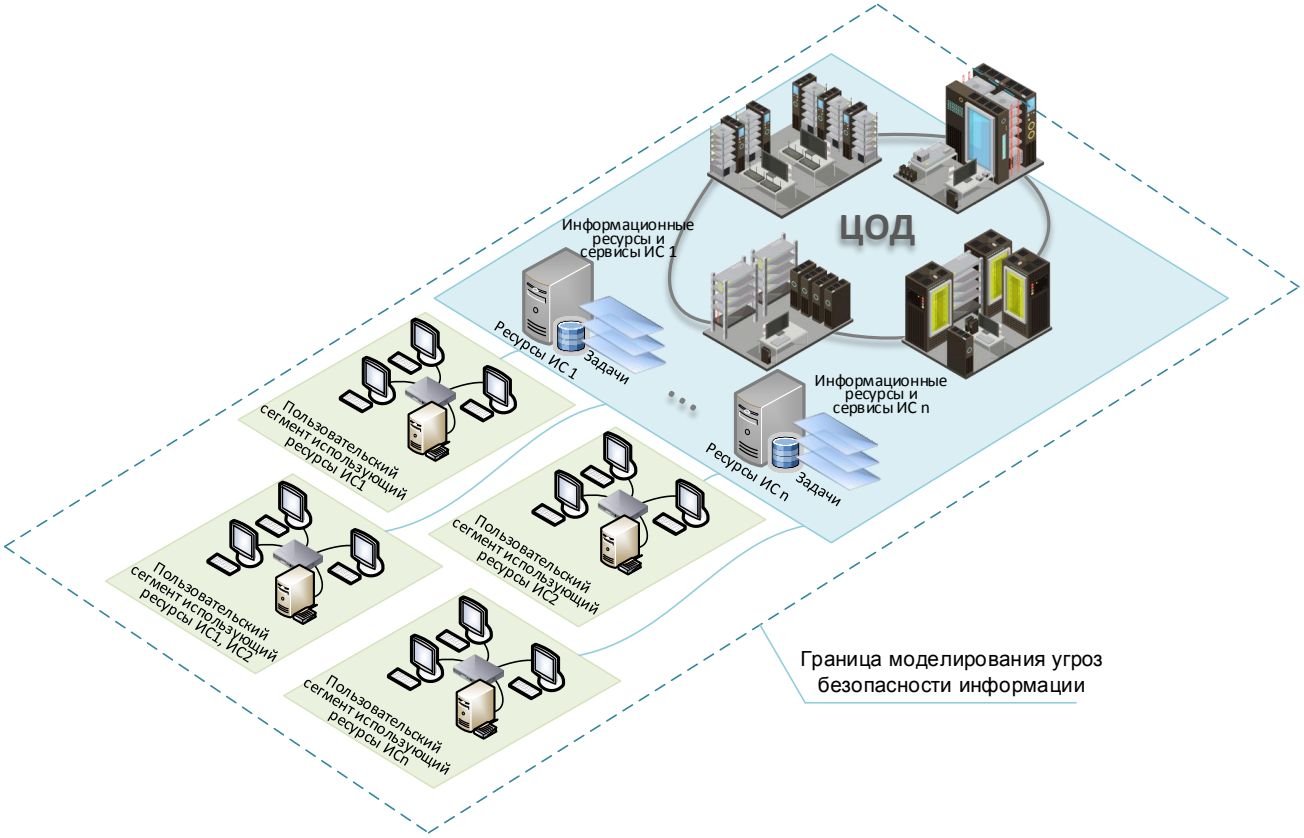

Рисунок 2 – Пример границы процесса моделирования угроз безопасности информации в информационной инфраструктуре на базе центра обработки данных

2.11. При размещении систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, принадлежащей поставщику услуг, моделирование угроз безопасности информации проводится оператором во взаимодействии с поставщиком услуг. Пример распределения зон ответственности между оператором и поставщиком услуг представлен на рисунке 3.

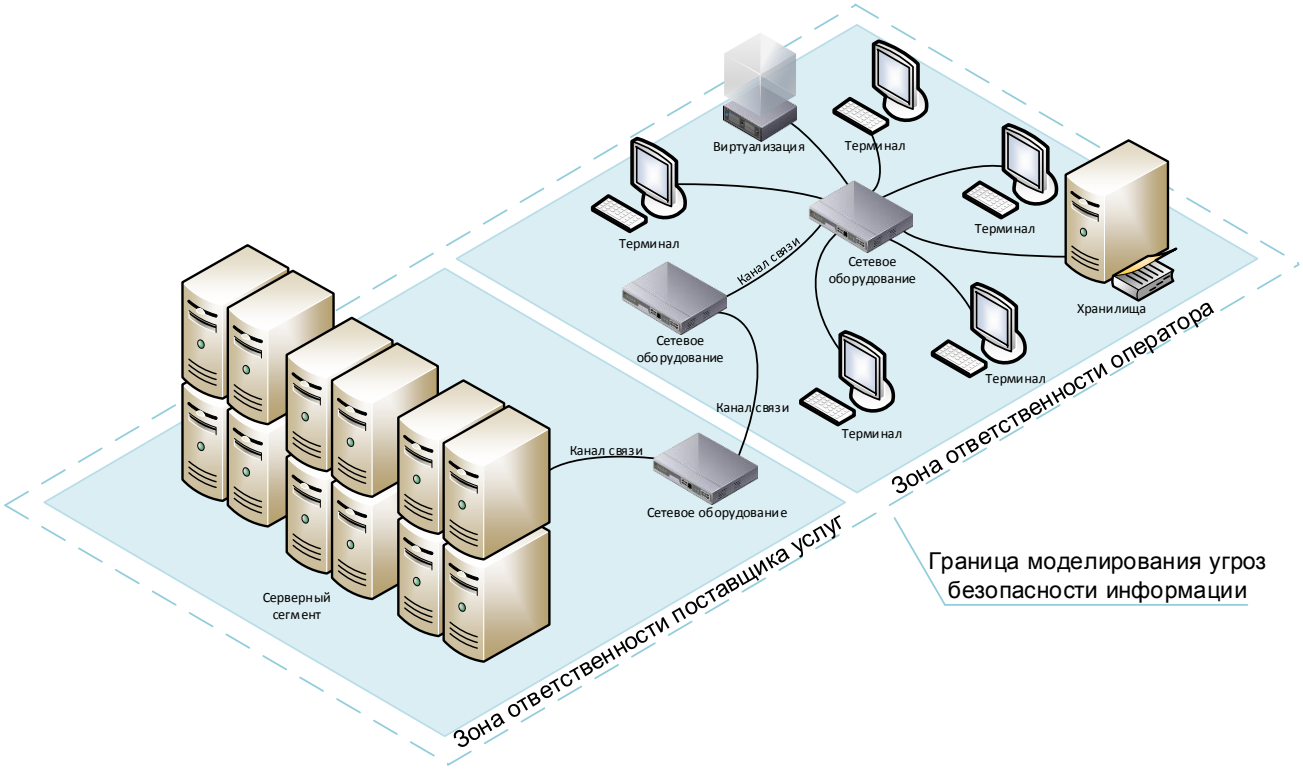

Рисунок 3 – Пример распределения зон ответственности между оператором и поставщиком услуг

Угрозы безопасности информации, актуальные для арендуемых компонентов информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, определяются поставщиком услуг в модели угроз безопасности информации информационно-телекоммуникационной инфраструктуры центра обработки данных (облачной инфраструктуры). Указанная модель угроз безопасности информации предоставляется оператору для использования в ходе моделирования угроз безопасности информации в принадлежащих ему системах и сетях.

Поставщик услуг информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры информирует оператора об изменении угроз безопасности информации в его информационно-телекоммуникационной инфраструктуре.

Если поставщик услуг не определил угрозы безопасности информации для информационно-телекоммуникационной инфраструктуры центра обработки данных (облачной инфраструктуры), размещение на базе такой инфраструктуры систем и сетей не рекомендуется.

2.12. При моделировании угроз безопасности информации в системах и сетях, функционирующих на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры,

учитываются состав и содержание услуг, предоставляемых поставщиком услуг (например, SaaS, PaaS, IaaS).

При аренде оператором вычислительных ресурсов (физических серверов, систем хранения данных и т.д.) арендуемые программно-аппаратные средства и все их физические и логические интерфейсы взаимодействия с информационно-телекоммуникационной инфраструктурой поставщика услуг включаются в границу процесса моделирования угроз безопасности информации, проводимой оператором. В отношении остальной информационно-телекоммуникационной инфраструктуры угрозы безопасности информации определяются поставщиком услуг (рисунок 4).

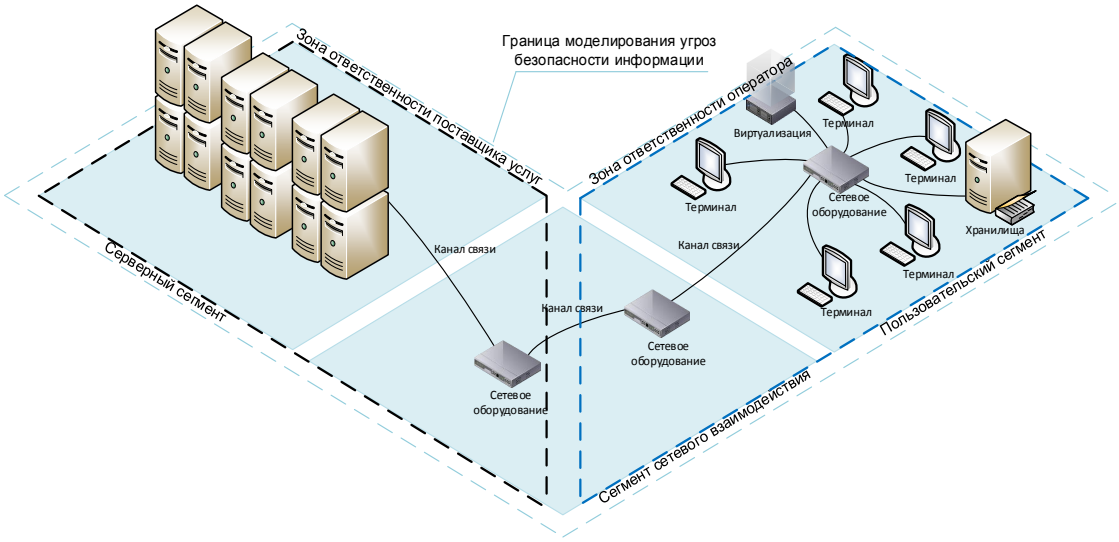

Рисунок 4 – Пример границы моделирования угроз безопасности информации в информационной инфраструктуре на базе центра обработки данных поставщика услуг

При аренде программного обеспечения (в том числе виртуальных машин, виртуальных серверов, систем управления виртуализацией, виртуальных каналов связи и т.д.) в границу моделирования угроз безопасности информации оператора включается арендуемое программное обеспечение, а также программные интерфейсы взаимодействия с иным программным обеспечением и программно-аппаратными средствами, на которых это программное обеспечение функционирует и с которыми взаимодействует. Моделирование угроз безопасности информации для программно-аппаратных средств, на которых функционирует программное обеспечение, осуществляется поставщиком услуг. Пример определения границы процесса моделирования угроз безопасности

информации для систем и сетей, функционирующих на базе средств виртуализации информационно-телекоммуникационной инфраструктуры центра обработки данных, арендованной оператором, приведен на рисунке 5.

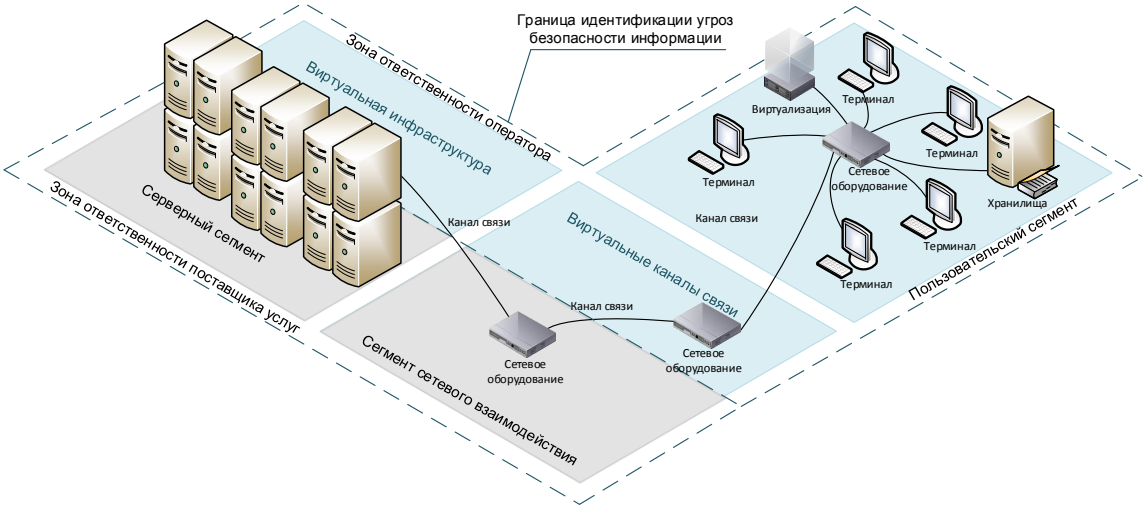

Рисунок 5 – Пример границы моделирования угроз безопасности информации при аренде виртуальной инфраструктуры

2.13. Результаты моделирования угроз безопасности информации отражаются в модели угроз, которая представляет собой формализованное описание актуальных угроз безопасности информации. Структура модели угроз безопасности информации приведена в приложении № 3 к настоящей Методике.

2.14. Модель угроз безопасности информации формируется применительно ко всем информационным ресурсам и компонентам систем и сетей, которые были включены в границу процесса моделирования угроз безопасности информации.

По решению обладателя информации (заказчика) или оператора модель угроз безопасности информации может разрабатываться для отдельной системы или сети. При этом модель угроз безопасности информации должна содержать описание угроз безопасности информации, актуальных для информационно-телекоммуникационной инфраструктуры, на базе которой эта система функционирует, а также угроз безопасности информации, связанных с интерфейсами взаимодействия со смежными (взаимодействующими) системами и сетями.

2.15. Модель угроз безопасности информации должна поддерживаться в актуальном состоянии в процессе функционирования систем и сетей.

Ведение модели угроз безопасности информации и поддержание ее в актуальном состоянии может осуществляться в электронном виде. При этом ее вид определяется обладателем информации или оператором с учетом приложения № 3 к настоящей Методике.

Изменение модели угроз безопасности информации осуществляется в случаях:

а) изменения требований нормативных правовых актов Российской Федерации и методических документов ФСТЭК России, регламентирующих вопросы моделирования угроз безопасности информации;

б) изменения архитектуры и условий функционирования систем и сетей, порядка обработки информации, влияющих на угрозы безопасности информации;

в) выявления, в том числе по результатам внешнего или внутреннего контроля эффективности защиты информации (аудита, тестирований на проникновение), новых угроз безопасности информации или новых сценариев реализации существующих угроз.

При проведении внутреннего или внешнего контроля эффективности защиты информации (аудита, тестирований на проникновение) перед организациями, проводящими такие работы, должна ставиться задача по выявлению максимально возможного числа сценариев реализации существующих угроз безопасности информации, а также задача выявления новых угроз безопасности информации, приводящих к наступлению негативных последствий.

3. ОПРЕДЕЛЕНИЕ ВОЗМОЖНЫХ НЕГАТИВНЫХ ПОСЛЕДСТВИЙ ОТ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

3.1. Возможные негативные последствия от реализации угроз безопасности информации определяются на основе требований законодательства Российской Федерации и (или) исходя из результатов проведенной обладателем информации (оператором) оценки ущерба (рисков) от нарушения основных (критических) процессов (бизнес-процессов) и (или) от нарушения безопасности обрабатываемой информации.

К негативным последствиям от реализации угроз безопасности относятся событие или группа событий, наступление которых в результате успешной реализации угроз безопасности может привести к нарушению законодательства Российской Федерации и (или) социальному, экономическому (финансовому), политическому, технологическому, экологическому ущербу, ущербу в области обеспечения обороны страны, безопасности государства и правопорядка, ущербу репутации или иным негативным последствиям, установленным законодательством Российской Федерации или определенным по результатам проведенной оценки ущерба (рисков).

Возможные негативные последствия должны быть конкретизированы применительно к областям и особенностям деятельности обладателя информации и оператора. Для систем и сетей обладателя информации (оператора) может быть определено одно или несколько негативных последствий.

Пример 2: *1) если оператор обрабатывает персональные данные граждан, которые в соответствии с Федеральным законом «О персональных данных» подлежат обязательной защите, одним из возможных негативных последствий от реализации угроз безопасности информации является утечка конфиденциальных персональных данных; 2) если оператор обеспечивает транспортировку нефти, одним из возможных негативных последствий от реализации угроз безопасности информации является загрязнение окружающей среды в результате разлива нефти из нефтепровода; 3) если оператор предоставляет услуги связи, одним из возможных негативных последствий от реализации угроз безопасности информации является непредставление услуг связи абонентам; 4) для оператора, который обеспечивает электроснабжение, в качестве одного из возможного негативного последствия от реализации угроз безопасности информации является нарушение электроснабжения потребителей; 5) для оператора по переводу денежных средств, одним из возможных негативных последствий от реализации угроз безопасности информации является хищение денежных средств*

В случае отсутствия на момент моделирования угроз безопасности информации результатов оценки ущерба (рисков) от нарушения основных (критических) процессов (бизнес-процессов) и (или) от нарушения безопасности обрабатываемой информации, угрозы могут определяться как на основе экспертной оценки специалистов, проводящих моделирование угроз безопасности информации, так и на основе информации, представляемой подразделениями, эксплуатирующими системы и сети.

3.2. В ходе определения возможности наступления негативных последствий от реализации угроз безопасности информации выявляются информационные ресурсы и (или) компоненты систем и сетей, обрабатывающие, хранящие информацию и (или) обеспечивающие реализацию основных (критических) процессов (бизнес-процессов), неправомерный доступ к которым и (или) воздействия на которые могут привести к наступлению негативных последствий, определенных в соответствии с пунктом 3.1 настоящей Методики. К таким информационным ресурсам и (или) компонентам систем и сетей относятся:

а) информация (данные), содержащаяся в системах и сетях;

б) программно-аппаратные средства (в том числе автоматизированные рабочие места, серверы, в том числе промышленные, машинные носители информации, телекоммуникационное оборудование и линии связи, средства отображения информации, программируемые логические контроллеры, производственное, технологическое оборудование (исполнительные устройства);

в) программные средства;

г) средства защиты информации;

д) обеспечивающие системы.

Информационные ресурсы и компоненты систем и сетей определяются в соответствии с их архитектурой на аппаратном, на системном и прикладном уровнях, на уровне сетевого взаимодействия, а также на уровне пользователей на основе изучения и анализа информации об архитектуре систем и сетей, их подсистем, логической структуры, видах обрабатываемой информации, информационных потоках между компонентами, картах сетей, описании внешних интерфейсов, API, сетевых потоков и иных сведений, представленных в документации (например, эскизный, технический проекты, технорабочий проект) на системы и сети.

3.3. Для каждого информационного ресурса и компонента систем и сетей обрабатывающего, хранящего информацию и (или) обеспечивающего реализацию

основных (критических) процессов (бизнес-процессов), должны быть определены виды неправомерного доступа и (или) воздействий, которые могут привести к наступлению негативных последствий, определенных в соответствии с пунктом 3.1 настоящей Методики.

Основными видами неправомерного доступа и (или) воздействий на информационные ресурсы и (или) компоненты систем и сетей являются:

а) утечка (нарушение конфиденциальности) защищаемой информации, системных, конфигурационных, иных служебных данных;

б) несанкционированный доступ к компонентам систем или сетей, защищаемой информации, системным, конфигурационным, иным служебным данным;

в) отказ в обслуживании отдельных компонентов или систем и сетей в целом;

г) модификация (подмена) защищаемой информации, системных, конфигурационных, иных служебных данных;

д) несанкционированное использование вычислительных ресурсов в интересах решения несвойственных задач;

е) нарушение функционирования (работоспособности) средств обработки и хранения информации.

Виды неправомерного доступа и (или) воздействий на информационные ресурсы и (или) компоненты систем и сетей должны быть конкретизированы применительно к архитектуре и условиям функционирования систем и сетей.

Пример 3: *1) утечка конфиденциальных персональных данных и (или) их модификация возможны в результате несанкционированного доступа к базе данных, в которой эта информация храниться; 2) разлив нефти из нефтепровода возможен в результате несанкционированного доступа к программируемому логическому контроллеру, обеспечивающему управление задвижками нефтепровода, и подмены хранящихся в нем значений уставок; 3) непредставление услуг связи абонентам возможно в результате отказа в обслуживании маршрутизатора уровня ядра сети; 4) нарушение электроснабжения потребителей возможно в результате несанкционированного доступа к программируемому логическому контроллеру, управляющему выключателем, с целью подачи ложных команд на его отключение; 5) хищение денежных средств у оператора по переводу денежных средств возможно в результате подмены (модификации) информации, содержащейся в электронных сообщениях*

3.4. В результате определения возможных негативных последствий от реализации угроз безопасности информации должны быть установлены:

а) перечень возможных негативных последствий, конкретизированный применительно к областям и особенностям деятельности обладателя информации и (или) оператора;

б) информационные ресурсы и компоненты систем и сетей, обрабатывающие, хранящие информацию и (или) обеспечивающие реализацию основных (критических) процессов (бизнес-процессов);

в) виды неправомерного доступа и (или) воздействий на информационные ресурсы и компоненты систем и сетей, которые могут привести к наступлению негативных последствий (угрозы безопасности информации).

Примеры определения возможных негативных последствий от реализации угроз безопасности информации приведены в таблице 1.

Таблица 1

Негативные последствия	**Информационные ресурсы, компоненты**	**Возможные угрозы безопасности информации**
Разглашение персональных данных граждан	База данных информационной системы, содержащая идентификационную информацию граждан	Несанкционированный доступ к серверу, на котором функционирует база данных. Утечка информации, содержащей идентификационную информацию граждан
	Линия связи между сервером основного центра обработки данных и сервером резервного центра обработки данных	Перехват (нарушение конфиденциальности) информации, содержащей идентификационную информацию граждан, передаваемой по линиям связи
	Удаленное автоматизированное рабочее место (АРМ) пользователя	Несанкционированный доступ к АРМ пользователя, с которого вводится идентификационная и аутентификационная информация. Нарушение конфиденциальности логина и пароля пользователя для удаленного доступа к своим персональным данным, хранящимся в базе данных
Загрязнение окружающей среды и водоемов в результате разлива нефти из нефтепровода	Коммутационный контроллер для управления аварийными задвижками в нефтепроводе	Перезапись регистров памяти коммутационного контроллера, приводящая к нарушению функционирования коммутационного контроллера.

Негативные последствия	Информационные ресурсы, компоненты	Возможные угрозы безопасности информации
		Подмена команд в пакетах промышленного протокола, приводящая к изменению параметров функционирования контроллера
	АРМ оператора	Несанкционированный доступ к АРМ оператора и несанкционированная отправка команд, приводящая к несрабатыванию средств аварийной защиты и изменению логики ПЛК
	Программируемый логический контроллер (ПЛК) для управления насосными станциями	Изменение логики и уставок в ПЛК, приводящее к несрабатыванию аварийных задвижек
Хищение денежных средств со счета организации	Банк-клиент	Подмена данных, содержащихся в реквизитах платежного поручения
	АРМ финансового директора организации	Модификация информации в платежных распоряжениях и отправка недостоверных распоряжений от имени финансового директора
	АРМ главного бухгалтера организации	Подмена данных, содержащих реквизиты платежных поручений и другой платежной информации, на АРМ главного бухгалтера
Срыв запланированной сделки с партнером	АРМ председателя совета директоров	Модифицирование информации и отправка электронных писем с недостоверной информацией от имени председателя совета директоров
Невозможность (прерывание) предоставления услуг (сервисов)	Веб-приложение (сайт) портала государственных услуг (сервисов)	Отказ в обслуживании веб-приложения. Нарушение логики работы веб-приложения
	Сервер баз данных портала государственных услуг (сервисов)	Отказ в обслуживании сервера баз данных. Подмена информации в базах данных на недостоверную информацию
Нарушение выборного процесса	Сервер баз данных с результатами голосования	Искажение информации в таблицах базы данных
Снижение показателей заказа в области обеспечения обороны страны, безопасности государства и правопорядка	Электронная торговая площадка для гособоронзаказа	Отказ в обслуживании электронной торговой площадки. Модифицирование информации о проводимых торгах на страницах веб-приложения

4. ОЦЕНКА УСЛОВИЙ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

4.1. При моделировании угроз безопасности информации на основе анализа архитектуры и условий функционирования систем и сетей должны быть оценены условия, которые может обладать нарушитель для реализации угроз безопасности информации.

4.2. Условиями, необходимыми для реализации угроз безопасности информации, являются:

а) наличие уязвимостей и (или) недекларированных возможностей в системах и сетях, использование которых возможно нарушителем;

б) наличия доступа к компонентам систем и сетей для реализации угроз безопасности информации.

4.3. При реализации угроз безопасности информации могут быть использованы уязвимости кода (программного обеспечения), уязвимости архитектуры и конфигурации систем и сетей, а также организационные уязвимости. При этом уязвимости кода, архитектуры и конфигурации могут использоваться в микропрограммном, общесистемном и прикладном программном обеспечении, телекоммуникационном оборудовании и в средствах защиты информации. Более высокие возможности нарушителя позволяют ему использовать уязвимости, которые являются более сложными с точки зрения их идентификации и использования.

Описание уязвимостей, которые могут быть использованы для реализации угроз безопасности информации, содержится в ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем».

4.4. Недекларированные возможности представляют собой потенциально опасные функциональные возможности средств обработки и хранения информации, которые могут быть использованы для реализации угроз безопасности информации. Реализация угроз безопасности информации, связанных с недекларированными возможностями, возможна нарушителями, имеющими необходимый уровень возможностей для их внедрения и использования. Недекларированные возможности могут быть внедрены непосредственно разработчиком этих средств или иными видами нарушителей на этапах разработки, производства, поставки или ремонта средств обработки и хранения информации.

4.5. При моделировании угроз безопасности информации на этапе создания систем и сетей оценивается наличие и возможность использования нарушителем потенциальных уязвимостей. Предположение о наличии потенциальных уязвимостей делается на основе анализа информации о типовых уязвимостях, ошибках, описаниях шаблонов атак, информации об эксплойтах, характерных для классов, типов и версий программного обеспечения, программно-аппаратных средств, средств защиты информации, применяемых (планируемых к применению) в системах и сетях.

4.6. При моделировании угроз безопасности информации на этапе эксплуатации систем и сетей возможность идентификации и использования уязвимости оценивается по результатам контроля защищенности систем и сетей (тестирований на проникновение), в том числе с учетом функциональных возможностей и настроек средств защиты информации. Вывод о возможности идентификации и использования уязвимостей делается, если по результатам экспертного анализа и (или) тестирований на проникновение подтверждена возможность их эксплуатации нарушителем.

4.7. В зависимости от архитектуры и условий функционирования систем и сетей для реализации угроз безопасности информации может быть использован удаленный, локальный или физический доступ к информационным ресурсам и (или) компонентам.

Удаленный доступ при реализации угроз безопасности информации осуществляется нарушителем из-за границы систем и сетей при их взаимодействии с сетями связи общего пользования, в первую очередь с сетью Интернет. При удаленном доступе воздействия на информационные ресурсы и компоненты систем и сетей реализуются посредством сетевых протоколов. При этом могут быть использованы сетевые протоколы на всех уровнях сетевой эталонной модели OSI.

Угрозы безопасности информации при удаленном доступе реализуются внешними нарушителями, не обладающими правами в системах и сетях (рисунок 6).

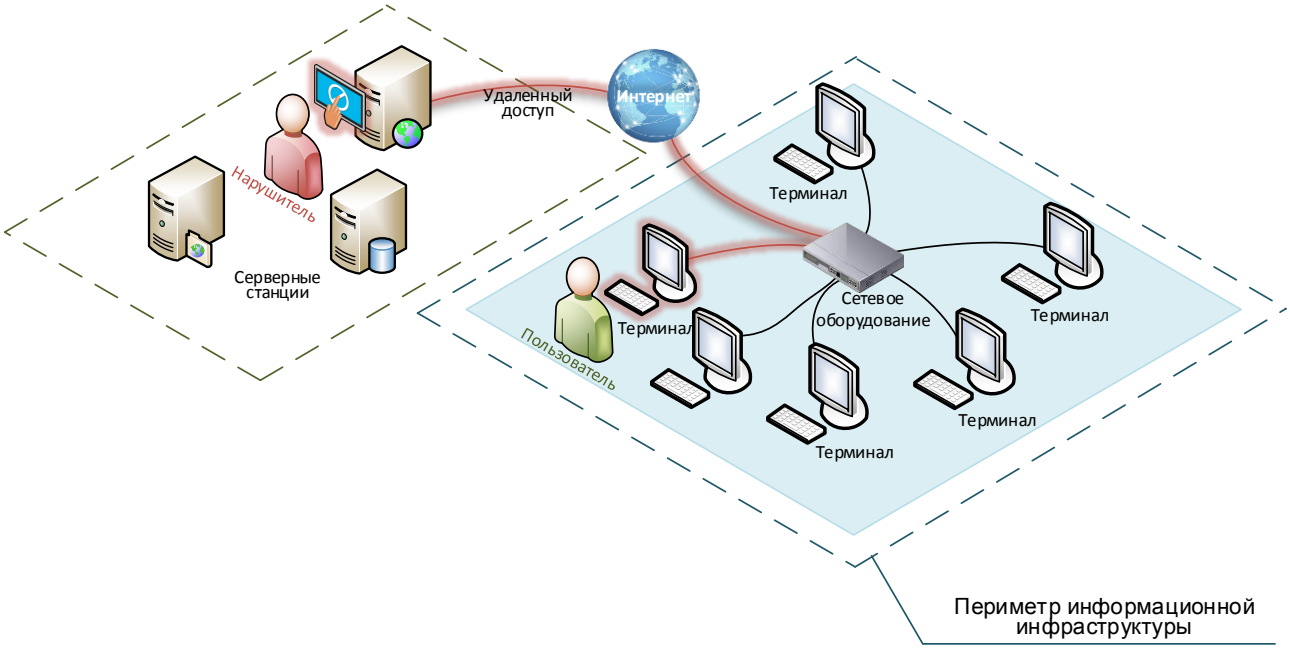

Рисунок 6 – Реализация угроз безопасности информации при удаленном доступе

Локальный доступ при реализации угроз безопасности информации может осуществляться нарушителем в пределах границ систем и сетей. При локальном доступе неправомерный доступ и (или) воздействие на информационные ресурсы и компоненты реализуются при наличии и использовании локальной учетной записи пользователя, зарегистрированной в системе или сети. Удаленное использование нарушителем локальной учетной записи пользователя, в том числе из взаимодействующей (смежной) системы или сети Интернет, при реализации угрозы безопасности информации относится к локальному доступу.

Угрозы безопасности информации при локальном доступе реализуются внутренними нарушителями или внешними в случае получения ими локального доступа (рисунок 7).

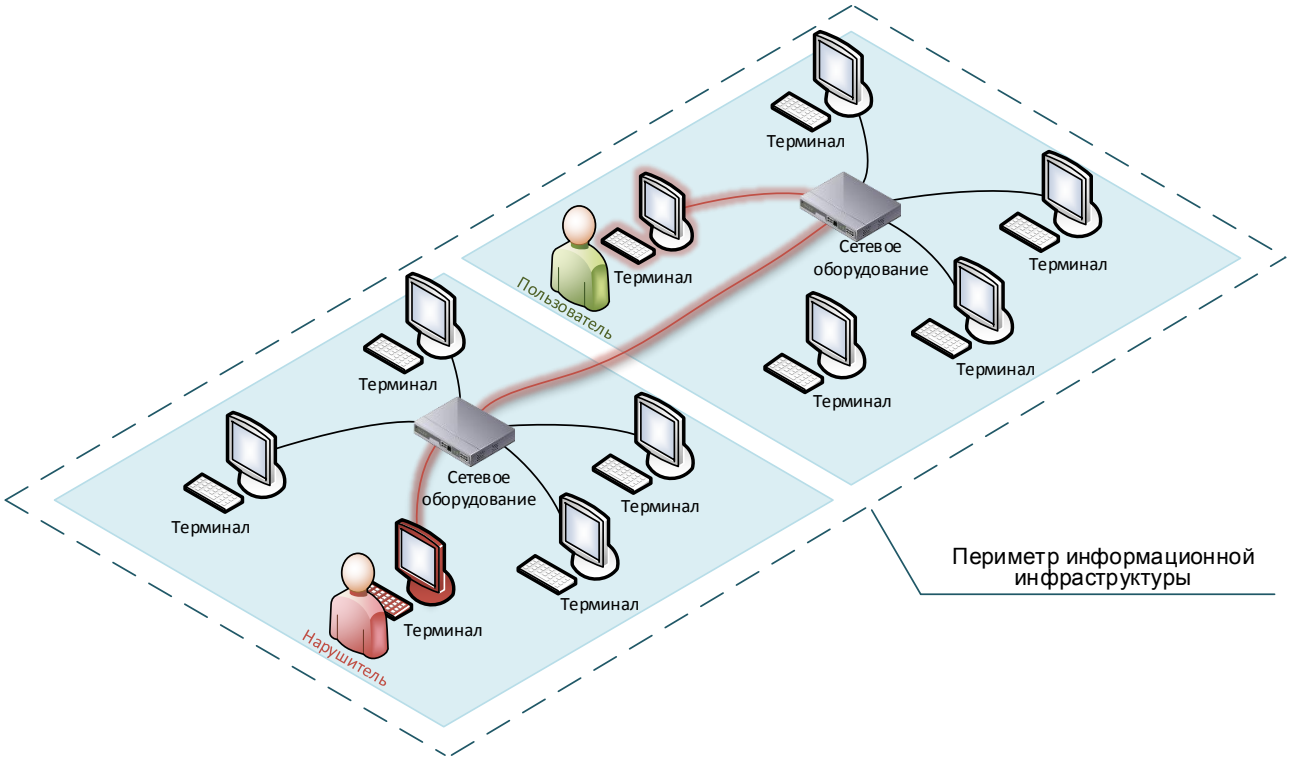

Рисунок 7 – Реализация угроз безопасности информации при локальном доступе

Физический доступ для реализации угроз безопасности информации может осуществляться нарушителями в пределах границ систем и сетей и при наличии у них непосредственного физического доступа к средствам обработки и хранения информации.

***Пример 4**: Основным отличием угроз безопасности информации, связанных с физическим доступом, от угроз безопасности информации, связанных с локальным доступом, является возможность реализации угроз без доступа к информационным ресурсам. Например, кража машинного носителя информации или физическое разрушение средств обработки или хранения информации, повлекшие нарушение функционирования систем и сетей.*

Целью физического доступа нарушителя также может являться получение локального доступа для реализации локальных угроз безопасности информации (рисунок 8). В этом случае оценке подлежат угрозы безопасности информации, связанные с локальным доступом к информационным ресурсам и компонентам систем и сетей.

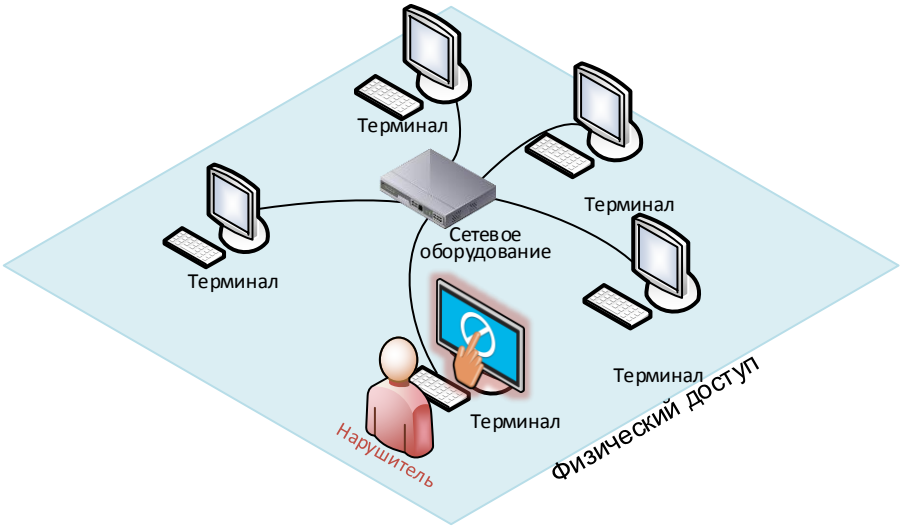

Рисунок 8 - Реализация угроз безопасности информации при физическом доступе

4.8. Для непреднамеренных угроз безопасности информации условием их возникновения является наличие у внутреннего нарушителя локального и (или) физического доступа к системам и сетям. При этом внутренний нарушитель может иметь привилегированные или непривилегированные права по доступу к информационным ресурсам и (или) компонентам систем и сетей.

4.9. По результатам оценки условий реализации угроз безопасности информации должны быть определены:

а) типы уязвимостей и (или) недекларированные возможности в компонентах систем и сетей, которые могут быть использованы нарушителем для реализации угроз безопасности информации;

б) варианты возможного доступа нарушителей к информационным ресурсам и компонентам систем и сетей для реализации угроз безопасности информации.

5. ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ОЦЕНКА ВОЗМОЖНОСТЕЙ НАРУШИТЕЛЕЙ

5.1. Источниками угроз безопасности информации для систем и сетей могут являться:

а) техногенные источники;

б) антропогенные источники.

При моделировании угроз безопасности информации оценке подлежат угрозы, связанные со всеми типами источников. В целях создания и эксплуатации адекватной эффективной системы защиты следует, в первую очередь, уделять внимание оценке антропогенных источников угроз, связанных с действиями нарушителей. Оценка возможностей нарушителей включает определение категорий, видов нарушителей, их компетенции и оснащенности, которыми они могут обладать для реализации угроз безопасности информации.

5.2. Возникновение угроз безопасности информации, связанных с техногенными источниками, возможно вследствие:

а) недостатков качества, надежности программного обеспечения, программно-аппаратных средств, обеспечивающих обработку и хранение информации, их линий связи (далее – средства обработки и хранения информации);

б) недостатков в работе обеспечивающих систем;

в) особенностей организации процессов у оператора (например, недостатки в организации работ по найму персонала, временные ограничения на реализацию мер);

г) недоступности сервисов, предоставляемых сторонними организациями;

д) недостатков гарантийного, технического обслуживания со стороны обслуживающих организаций и лиц, ошибок, допущенных при таком обслуживании.

Источниками техногенных угроз безопасности информации также могут быть природные явления (землетрясения, осадки, недопустимые температурные режимы), если в результате их возникновения возможно нарушение функционирования средств обработки и хранения информации и (или) обеспечивающих систем.

Угрозы безопасности информации, связанные с техногенными источниками, включаются в модель угроз, если к системам и сетям предъявлены требования к устойчивости и надежности функционирования. Негативными последствиями от возникновения угроз безопасности информации, связанных с

техногенными источниками, являются нарушение или прекращение функционирования систем и сетей, их отдельных компонентов или обеспечивающих систем. Возможность возникновения таких угроз определяется на основе статистики их возникновения за прошлые годы. В случае отсутствия указанной статистики возможно использование экспертного метода оценки.

5.3. Источником антропогенных угроз безопасности информации является лицо (группа лиц), осуществляющее реализацию угроз безопасности информации путем несанкционированного доступа и (или) воздействий на информационные ресурсы и (или) компоненты систем и сетей.

Действия по реализации угроз безопасности информации могут осуществляться нарушителем преднамеренно (преднамеренные угрозы безопасности информации) или непреднамеренно (непреднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых.

Отдельные угрозы безопасности информации могут быть реализованы опосредованно за счет внедрения программных, программно-аппаратных или аппаратных закладок. Если угроза безопасности информации может быть реализована за счет внедрения программной, программно-аппаратной или аппаратной закладки, функционирование которой не требует участия нарушителя, в качестве источника угрозы безопасности информации может рассматриваться как лицо, внедрившее закладку, так и непосредственно закладка.

***Пример 5**: для несанкционированного доступа к данным о конфигурации программного обеспечения и вывода сведений об этом из системы может быть использована программная закладка. В случае невозможности установления категории и вида нарушителя, внедрившего программную закладку, в качестве источника данной угрозы рассматривается непосредственно программная закладка*

5.4. В зависимости от имеющихся прав и возможностей нарушители подразделяются на две категории:

внешние нарушители – субъекты, не имеющие полномочий по доступу к информационным ресурсам и компонентам систем и сетей;

внутренние нарушители – субъекты, имеющие полномочия по доступу к информационным ресурсам и компонентам систем и сетей.

Внешние нарушители являются актуальными, когда системы и сети имеют взаимодействие с сетью Интернет или смежными (взаимодействующими) системами и сетями, в том числе посредством использования съемных машинных носителей информации, а также в случаях, когда имеется возможность физического доступа к средствам обработки и хранения информации, их линиям связи, расположенным вне контролируемой (охраняемой) зоны (территории) (рисунок 9).

***Пример 6**: 1) внешнего нарушителя в качестве актуального необходимо рассматривать в случаях, если имеется возможность доступа нарушителя к незащищенным линиям связи информационно-телекоммуникационной сети, проложенных в общих коммутационных каналах за пределами контролируемой (охраняемой) зоны (территории), или средствам обработки и хранения информации, расположенным вне контролируемой (охраняемой) зоны (территории); 2) внешний нарушитель является актуальным, если для обработки информации в изолированных системах и сетях применяются съемные машинные носители информации, которые одновременно используются для обработки, хранения, переноса информации из сети Интернет или смежных (взаимодействующих) систем и сетей*

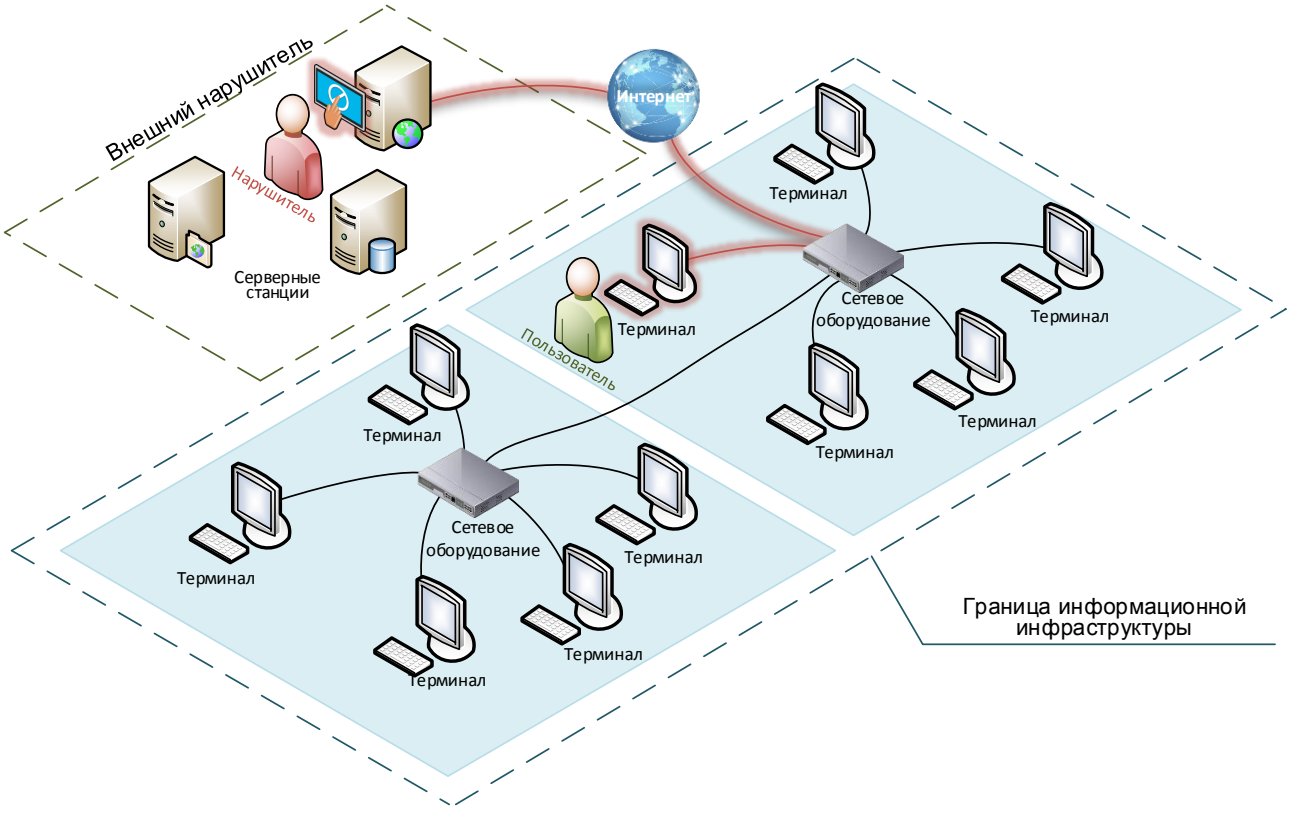

Рисунок 9 – Внешний нарушитель при реализации угроз безопасности информации

Внешний нарушитель, получивший в результате реализации угроз безопасности информации полномочия по доступу к компонентам систем и сетей, при дельнейшей оценке рассматривается как внешний нарушитель с возможностями внутреннего нарушителя.

В качестве внутренних нарушителей в системах и сетях должны рассматриваться пользователи, имеющие полномочия по доступу к информационным ресурсам и компонентам систем и сетей, а также персонал, обеспечивающий их функционирование (например, персонал, обеспечивающий гарантийную, техническую поддержку, ремонт, восстановление после сбоев, настройку). К внутренним нарушителям относятся пользователи, имеющие как непривилегированные (пользователи), так и привилегированные (администраторы) права доступа к компонентам систем и сетей (рисунок 10).

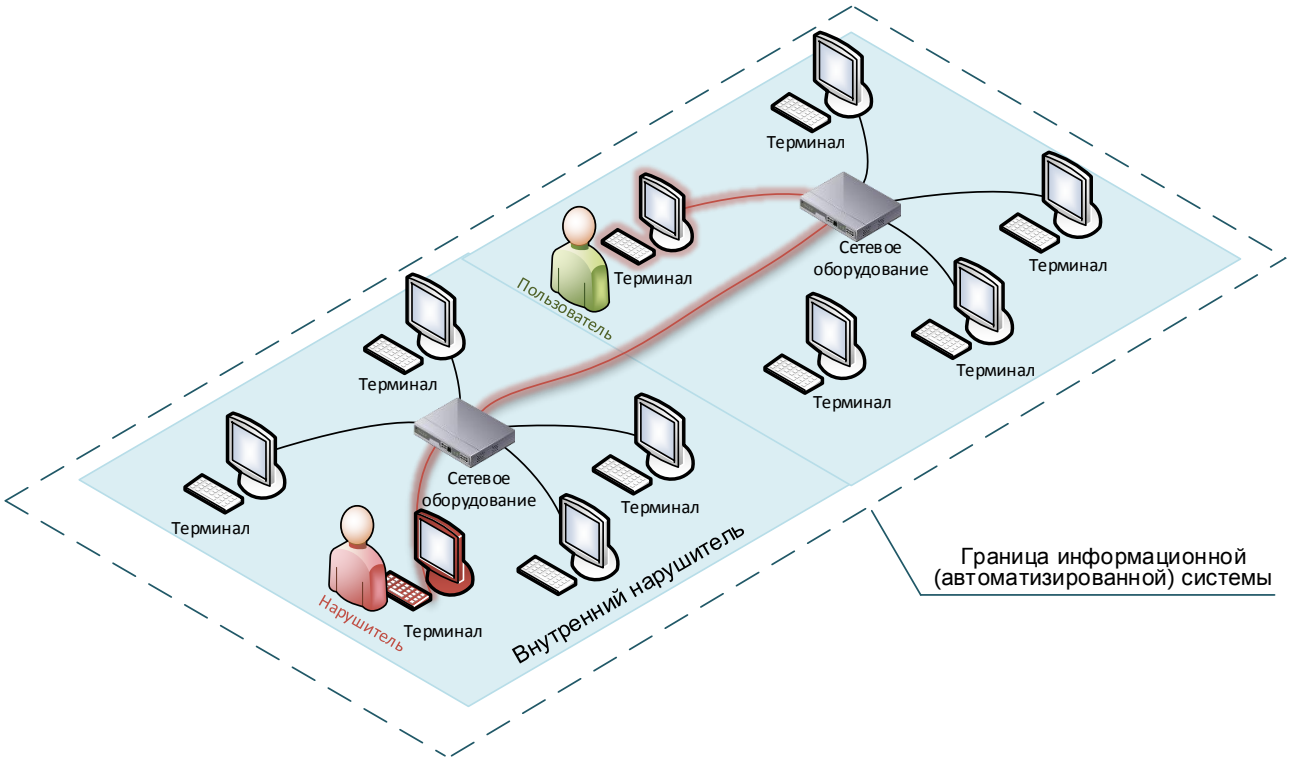

Рисунок 10 – Внутренний нарушитель при реализации угроз безопасности информации

5.5. Для каждой из категорий нарушителей, актуальных для систем и сетей, должны быть определены виды нарушителей и их возможности по реализации угроз безопасности информации. Виды нарушителей определяются на основе предположений о возможных целях реализации этими нарушителями угроз безопасности информации, которые зависят от назначения систем и сетей, выполняемых ими функций и решаемых с их использованием задач, а также

значимости обрабатываемой информации. Возможные цели нарушителя при реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности приведены в таблице 2.

Таблица 2

№ п/п	Возможные цели реализации угроз безопасности информации	Виды нарушителя	Уровень возможностей нарушителя (потенциал)
1.	Нанесение ущерба государству, отдельным его сферам (областям) деятельности или секторам экономики	Специальные службы иностранных государств	Высокий
2.	Нарушение или прекращение функционирования, дискредитация деятельности органов государственной власти, корпораций, организаций	Специальные службы иностранных государств	Высокий
		Террористические, экстремистские организации	Средний
3.	Публикация недостоверной социально значимой информации на веб-ресурсах организации, которая может привести к социальной напряженности, панике среди населения и т.п.	Специальные службы иностранных государств	Базовый повышенный
4.	Нарушение работоспособности систем и сетей органов государственной власти, предприятий оборонно-промышленного комплекса	Специальные службы иностранных государств	Высокий
		Террористические, экстремистские организации	Средний
5.	Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса, если это ведет к выводу из строя технологических объектов, их компонент или к техногенным авариям	Специальные службы иностранных государств	Высокий
		Террористические, экстремистские организации	Средний
6.	Доступ к персональным данным сотрудников органов государственной власти, уполномоченных в области обеспечения обороны, безопасности и правопорядка, высших должностных лиц государственных органов и других лиц государственных органов	Специальные службы иностранных государств	Высокий
		Террористические, экстремистские организации	Средний
7.	Публикация недостоверной информации на веб-ресурсах организации	Преступные группы	Базовый повышенный
8.	Использование веб-ресурсов для распространения и управления вредоносным программным обеспечением	Преступные группы	Базовый повышенный
9.	Искажение информации для получения финансовой выгоды	Преступные группы	Базовый повышенный

№ п/п	Возможные цели реализации угроз безопасности информации	Виды нарушителя	Уровень возможностей нарушителя (потенциал)
10.	Тестирование хакерских инструментов или апробация описанных способов осуществления атак	Физические лица	Базовый
11.	Рассылка информационных сообщений с использованием вычислительных мощностей оператора и(или) от его имени	Преступные группы	Базовый повышенный
12.	Получение доступа к системам и сетям с целью незаконного использования вычислительных мощностей	Преступные группы	Базовый повышенный
13.	Получение доступа к системам и сетям с целью дальнейшей продажи доступа	Преступные группы	Базовый повышенный
14.	Получение преимущества за счет нарушения работоспособности систем и сетей	Конкурирующие организации	Базовый повышенный
15.	Нарушение работоспособности систем и сетей по причинам личной неприязни	Физические лица	Базовый
16.	Хищение денежных средств	Преступные группы	Базовый повышенный
17.	Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса	Конкурирующие организации	Базовый повышенный
18.	Внедрение скрытых функций в продукцию на этапе разработки, производства, поставки	Специальные службы иностранных государств	Высокий
		Разработчики, производители, поставщики программных, программно-аппаратных средств	Средний
19.	Внедрение скрытых функций в компоненты систем и сетей на этапе эксплуатации, ремонта	Лица, привлекаемые для ремонта, регламентного обслуживания и иных работ	Базовый повышенный
20.	Кража конфиденциальной информации	Преступные группы	Базовый повышенный
		Конкурирующие организации	Базовый повышенный
		Лица, привлекаемые для администрирования (управления)	Базовый повышенный
		Лица, привлекаемые для ремонта, регламентного	Базовый повышенный

№ п/п	Возможные цели реализации угроз безопасности информации	Виды нарушителя	Уровень возможностей нарушителя (потенциал)
		обслуживания и иных работ	
		Лица, обеспечивающие функционирование или обслуживание обеспечивающих систем, уборку, охрану	Базовый
		Отдельные физические лица (хакеры)	Базовый
		Пользователи (привилегированные, непривилегированные)	Базовый
21.	Непреднамеренные, неосторожные или неквалифицированные действия	Лица, привлекаемые для ремонта, регламентного обслуживания и иных работ	Базовый повышенный
		Лица, обеспечивающие функционирование или обслуживание обеспечивающих систем, уборку, охрану	Базовый повышенный
		Пользователи (привилегированные, непривилегированные)	Базовый
		Лица, привлекаемые для администрирования (управления)	Базовый
22.	Незаконное обогащение путем вымогательства денежных средств за восстановление доступа к заблокированным данным	Преступные группы	Базовый повышенный

Для одной системы или сети актуальными могут являться нарушители нескольких видов с разными уровнями возможностей (потенциала). При этом меры по защите информации (обеспечению безопасности) в системах и сетях принимаются в соответствии с уровнями возможностей актуальных нарушителей.

***Пример 7**: 1) для государственной информационной системы, в которой обрабатывается информация о состоянии бюджета бюджетной системы, актуальными нарушителями могут являться как специальные службы, так и отдельные физические лица; 2) для информационной системы, обрабатывающей персональные данные сотрудников правоохранительных органов, актуальными нарушителями могут являться террористические, экстремистские организации, преступные группы, которые обладают разными уровнями возможностей*

При определении видов нарушителей, актуальных для систем и сетей, отдельные виды нарушителей могут быть исключены из рассмотрения, если у обладателя информации и (или) оператора в соответствии с законодательством Российской Федерации принимаются правовые, организационные или иные меры, исключающие возможность реализации им угроз безопасности (например, проверочные мероприятия, использование полиграфа).

5.6. Возможности (потенциал) нарушителей определяются компетентностью и оснащенностью, требуемыми им для реализации угроз безопасности информации. Уровни возможностей (потенциала) нарушителей приведены в таблице 3.

Таблица 3

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации
Н1	Нарушитель, обладающий базовыми возможностями (потенциалом)	Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети Интернет и разработанные другими лицами, имеют минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. Обладает базовыми компьютерными знаниями и навыками на уровне пользователя. **Таким образом, нарушители с базовыми возможностями (потенциалом) имеют возможность реализовывать только известные угрозы и компьютерные атаки, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов**
Н2	Нарушитель, обладающий базовыми повышенными возможностями (потенциалом)	Обладает всеми возможностями нарушителей с базовыми возможностями. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети Интернет и разработанные другими лицами, однако хорошо владеют этими средствами и инструментами, понимают, как они работают и могут вносить изменения в их функционирование для повышения эффективности реализации угроз. Хорошо владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. Имеет навыки самостоятельного планирования и реализации угроз безопасности информации. Обладает практическими знаниями о функционировании систем и сетей, операционных систем, а также имеют знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации
		Таким образом, нарушители с базовыми повышенными возможностями (потенциалом) имеют возможность реализовывать сценарии угроз и компьютерные атаки, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети Интернет. Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей
Н3	Нарушитель, обладающий средними возможностями (потенциалом)	Обладает всеми возможностями нарушителей с базовыми повышенными возможностями. Имеет возможность приобретать информацию об уязвимостях, размещаемую на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность приобретать дорогостоящие средства и инструменты для реализации угроз, размещаемую на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность самостоятельно разрабатывать средства (инструменты), необходимые для реализации угроз (атак), реализовывать угрозы с использованием данных средств. Имеет возможность получения доступа к встраиваемому программному обеспечению аппаратных платформ, системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-аппаратным средствам для проведения их анализа. Обладает знаниями и практическими навыками проведения анализа программного кода для получения информации об уязвимостях. Обладает высокими знаниями и практическими навыками о функционировании систем и сетей, операционных систем, а также имеют глубокое понимание защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. Имеет возможность реализовывать угрозы безопасности информации в составе группы лиц **Таким образом, нарушители со средними возможностями (потенциалом) имеют возможность реализовывать сценарии угроз и компьютерные атаки, в том числе на выявленные ими неизвестные уязвимости, с использованием самостоятельно разработанных для этого инструментов. Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей**
Н4	Нарушитель, обладающий высокими возможностями (потенциалом)	Обладают всеми возможностями нарушителей со средними возможностями. Имеет возможность получения доступа к исходному коду встраиваемого программного обеспечения аппаратных платформ, системного и прикладного программного обеспечения, телекоммуникационного оборудования и других программно-аппаратных средств для получения сведений об уязвимостях «нулевого дня». Имеет возможность внедрения программных (программно-аппаратных) закладок или уязвимостей на различных этапах

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации
		поставки программного обеспечения или программно-аппаратных средств. Имеет возможность создания методов и средств реализации угроз с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение. Имеет возможность реализовывать угрозы с привлечением специалистов, имеющих базовые повышенные, средние и высокие возможности. Имеет возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений. Имеет возможность долговременно и незаметно для операторов систем и сетей реализовывать угрозы безопасности информации. Обладает исключительными знаниями и практическими навыками о функционировании систем и сетей, операционных систем, аппаратном обеспечении, а также осведомлены о конкретных защитных механизмах, применяемых в программном обеспечении, программно-аппаратных средствах атакуемых систем и сетей **Таким образом, нарушители с высокими возможностями (потенциалом) имеют практически неограниченные возможности реализовывать сценарии угроз и компьютерные атаки, в том числе с использованием недекларированных возможностей, программных, программно-аппаратных закладок, встроенных в компоненты систем и сетей**

5.7. По результатам определения источников угроз безопасности информации и оценки возможностей нарушителей должны быть установлены:

а) источники угроз безопасности информации;

б) возможные цели реализации угроз безопасности информации нарушителями;

в) категории и виды нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы (актуальные нарушители);

г) возможности каждого вида нарушителей по реализации угроз безопасности информации в соответствии с имеющимися для этого условиями.

6. ОПРЕДЕЛЕНИЕ СЦЕНАРИЕВ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

6.1. Возможность реализации угрозы безопасности информации определяется наличием хотя бы одного сценария ее реализации.

Для построения эффективной системы защиты систем и сетей необходимо определение максимально возможного количества сценариев реализации угроз безопасности информации, реализуемых актуальными нарушителями, исходя из имеющихся у них для этого условий.

6.2. Определение сценариев реализации угроз безопасности информации предусматривает установление совокупности всех возможных тактик и техник (способов), применяемых нарушителями для неправомерного доступа и (или) воздействий на информационные ресурсы и компоненты систем и сетей.

Основные тактики и соответствующие им техники (способы), использование которых возможно нарушителем при реализации угроз безопасности информации, приведены в таблице 4.

Таблица 4

№	Тактика (тактическая задача)	Основные техники (способы) (технические действия)
Т1	Сбор информации о системах и сетях	Т1.1. Сбор информации об идентификаторах (логинах) пользователей
		Т1.2. Сканирование сетевых служб с целью определения уязвимостей, имеющих эксплойты или иные техники использования уязвимостей
		Т1.3. Поиск информации в файлах и каталогах, включая хэши паролей учётных записей
		Т1.4. Сбор инвентаризационной информации о компонентах систем и сетей
		Т1.5. Сбор конфигурационной информации о компонентах систем и сетей с целью выявления небезопасных конфигураций
Т2	Получение первоначального доступа к компонентам систем и сетей	Т2.1. Эксплуатация уязвимостей общедоступных компонентов систем и сетей с целью получения непосредственного доступа или внедрения средств получения аутентификационной информации (например, кейлогеров)
		Т2.2. Использование методов социальной инженерии
		Т2.3. Несанкционированное подключение внешних устройств

№	Тактика (тактическая задача)	Основные техники (способы) (технические действия)
		Т2.4. Использование доступа к системам и сетям, предоставленного сторонним организациям
		Т2.5. Использование доверенного доступа третьей доверенной стороны (поставщики ИТ-услуг, поставщики услуг безопасности)
		Т2.6. Подбор (методами прямого перебора, словарных атак, паролей производителей по умолчанию, рассеивания пароля, применения «радужных» таблиц) или компрометация легитимных учетных данных
		Т2.7. Использование программных, программно-аппаратных закладок
		Т2.8. Дарение носителей информации (например, флэш), содержащих вредоносное программное обеспечение
Т3	Внедрение и исполнение вредоносного программного обеспечения в системах и сетях	Т3.1. Запуск исполняемых скриптов и файлов
		Т3.2. Перенос вредносного кода через общие области памяти
		Т3.3. Выполнение кода через различного рода загрузчики
		Т3.4. Выполнение кода с помощью эксплоитов
		Т3.5. Подключение и запуск кода через интерфейсы удаленного управления
		Т3.6. Подмена легитимных программ и библиотек
		Т3.7. Создание скрипта при помощи доступного инструментария
		Т3.8. Запуск программ через планировщики и методы проксирования
		Т3.9. Подмена легитимных программ и библиотек под видом удалённых обновлений с портала производителя
		Т3.10. Подмена дистрибутивов (установочных комплектов) программ
Т4	Закрепление (сохранение доступа) в системе или сети	Т4.1. Несанкционированное создание учетных записей или кража существующих учетных данных
		Т4.2. Скрытая установка и запуск средств удаленного доступа
		Т4.3. Внесение в конфигурацию атакуемой системы или сети изменений, с помощью которых становится возможен многократный запуск вредоносного кода
		Т4.4. Маскирование подключённых устройств под легитимные (например, нанесение корпоративного логотипа, инвентарного номера, телефона службы поддержки)

№	Тактика (тактическая задача)	Основные техники (способы) (технические действия)
		Т4.5. Внесение соответствующих записей в реестр, автозагрузку, планировщики заданий, обеспечивающих запуск вредоносного программного обеспечения при перезагрузке системы или сети
Т5	Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ	Т5.1. Управление через стандартные протоколы (например, RDP, SSH)
		Т5.2. Управление через съемные носители
		Т5.3. Проксирование трафика управления
		Т5.4. Запасные и многоступенчатые каналы
		Т5.5. Использование штатных средств удаленного доступа и управления
		Т5.6. Туннелирование трафика управления в легитимные протоколы (например, DNS)
		Т5.7. Управление через подключённые устройства
Т6	Повышение привилегий по доступу компонентам систем и сетей	Т6.1. Подмена учетных данных
		Т6.2. Кража/перехват учетных данных
		Т6.3. Подбор параметров учетных данных
		Т6.4. Компрометация (захват) со стороны скомпрометированного компонента иных компонентов систем и сетей (например, AD), позволяющих повысить полномочия
Т7	Сокрытие действий и применяемых при этом средств от обнаружения	Т7.1. Очистка/затирание истории команд и журналов регистрации
		Т7.2. Подписание кода
		Т7.3. Манипуляции параметрами доступа (запуска процессов)
		Т7.4. Подмена прошивок
		Т7.5. Установление ложных доверенных отношений
		Т7.6. Отключение средств защиты (например, механизмов аудита, консолей оператора мониторинга)
		Т7.7. Удаление файлов
		Т7.8. Создание скрытых файлов/пользователей
		Т7.9. Модификация вредоносного программного обеспечения для удаления идентификаторов
		Т7.10. Маскировка вредоносного программного обеспечения под легитимные компоненты
		Т7.11. Обфускация файлов или информации
		Т7.12. Туннелирование управляющего трафика в легитимные протоколы
		Т7.13. Шифрование управляющего трафика
		Т7.14. Организация DoS-атак для невозможности получения журналов регистрации

№	Тактика (тактическая задача)	Основные техники (способы) (технические действия)
		Т7.15. Перенаправление журналов аудита (например, syslog) в нецелевую систему
		Т7.16. Организация переполнения хранилищ большим объёмом «мусорной» информации для невозможности дальнейшей записи событий аудита
Т8	Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям	Т8.1. Применение эксплойтов
		Т8.2. Использование средств и интерфейсов удаленного управления
		Т8.3. Использование механизмов дистанционной установки
		Т8.4. Удаленное копирование файлов
		Т8.5. Использование съемных носителей
		Т8.6. Итерация (повторение) техник из тактик №№ 1-3
Т9	Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз	Т9.1. Туннелирование выводимой информации в легитимные протоколы (например, DNS)
		Т9.2. Отправка данных по протоколам управления и функционирования
		Т9.3. Отправка данных по собственным протоколам
		Т9.4. Отправка данных через альтернативную среду
		Т9.5. Шифрование выводимой информации
		Т9.6. Вывод информации через разрешённые на периметровых средствах защиты стандартные tcp/udp-порты (например, tcp/80)
Т10	Неправомерный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящее к негативным последствиям	Т10.1. Доступ к памяти
		Т10.2. Доступ к системному программному обеспечению
		Т10.3. Доступ к прикладному программному обеспечению
		Т10.4. Права в приложение
		Т10.5. Локальный доступ
		Т10.6. Подмена информации (например, платёжных реквизитов)
		Т10.7. Уничтожение информации
		Т10.8. Добавление информации (например, дефейсинг корпоративного портала, публикация ложной новости)
		Т10.9. Организация отказа в обслуживании
		Т10.10. Организация майнинговой платформы, или платформы для осуществления атак на смежные (взимодействующие) системы и сети (например, DoS-атаки, подбор паролей)

При моделировании угроз безопасности информации проводится оценка возможности реализации нарушителем тактик и соответствующих им техник (способов), приведенных в таблице 4, и иных тактик и техник, включенных в банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru) или иные доступные базы данных компьютерных атаках.

При выявлении новых угроз безопасности информации или новых сценариев реализации существующих угроз, которые не приведены в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), рекомендуется направлять информацию о вновь выявленных тактиках и техниках реализации угроз безопасности информации в ФСТЭК России для актуализации банка данных угроз.

6.4. Сценарии реализации конкретных угроз безопасности информации могут не содержать все тактики и техники (способы), а предусматривать применение только отдельных из них, требуемых для успешной реализации угроз безопасности информации. Отдельные тактики и техники (способы) и их последовательность, используемые нарушителем при реализации угроз безопасности информации, могут повторяться.

***Пример 8**: 1) для успешной реализации угрозы отказа в облуживании достаточно исследовать атакуемую информационную систему с целью получения сведений о ее архитектуре, телекоммуникационном оборудовании и используемых сетевых протоколах. В этом случае повышать привилегии и обходить систему защиты информации не требуется; 2) нарушитель нашел несколько уязвимостей и пытается их эксплуатировать разными способами и с использованием разных средств, и успешной оказывается только третья попытка*

6.5. При определении тактик и техник (способов), которые могут быть задействованы нарушителем при реализации угроз безопасности информации, должны быть учтены типы доступа к компонентам систем и сетей, которыми может обладать нарушитель. Тип доступа определяет начальные тактики Т1 и Т2 сценариев реализации угроз безопасности.

6.6. В зависимости от категории, вида и возможностей нарушителей при реализации угроз безопасности информации тактики и техники (способы) могут быть реализованы на следующих уровнях:

на аппаратном уровне (объектами воздействия могут являться встраиваемое программное обеспечение, интегральные микросхемы, электрические схемы и цепи, интерфейсы аппаратного обеспечения, данные, иные компоненты);

на системном уровне (объектами воздействия могут являться гипервизоры, операционные системы, иные программы с системными привилегиями, информация, иные компоненты);

на прикладном уровне (объектами воздействия могут являться системы управления базами данных, браузеры, web-приложения, иные прикладные программы, информация, иные компоненты);

на сетевом уровне (объектами воздействия могут являться телекоммуникационное оборудование, линии связи, протоколы, иные компоненты);

на уровне сервисов (объектами воздействия являются пользователи, web-интерфейсы, информация, иные компоненты).

***Пример 9**: 1) нарушителями, обладающими базовыми возможностями, используются техники, связанные с эксплуатацией общеизвестных уязвимостей прикладного или системного уровней; 2) нарушителями, обладающими высокими возможностями, могут использоваться техники, связанные с эксплуатацией недекларированных возможностей в средствах обработки и хранения информации*

6.7. При моделировании непреднамеренных угроз безопасности информации определение сценариев возникновения угроз безопасности информации заключается в выявлении событий, наступление которых может способствовать реализации неправомерных действий в отношении систем и сетей и их компонентов. В этом случае исключаются действия нарушителя, связанные с преднамеренным воздействием на информационные ресурсы и компоненты систем и сетей.

6.8. По результатам определения сценариев реализации угроз безопасности информации для каждой i-ой угрозы безопасности информации ($УБИ_i$) формируется перечень возможных сценариев j ее реализации. Одна угроза безопасности информации ($УБИ_i$) может быть реализована j-м количеством сценариев ее реализации, отличающихся друг от друга компонентами или информационными ресурсами и видами неправомерного доступа или воздействий на них.

Сценарий реализации одной угрозы безопасности информации может включать сценарии реализации нескольких угроз безопасности информации, которые создают условия для реализации рассматриваемой угрозы.

Угроза безопасности информации (i) является актуальной, если имеется источник угрозы, условия для реализации угрозы, существует хотя бы один сценарий (j) ее реализации, а воздействие на информационные ресурсы или компоненты может привести к негативным последствиям.

$УБИ_{ij}$ = [источник угрозы; условия реализации, сценарий реализации $угрозы_j$; негативные последствия].

В качестве исходного перечня при идентификации угроз безопасности информации применяется банк данных угроз безопасности ФСТЭК России (bdu.fstec.ru), типовые и базовые модели угроз безопасности информации для различных классов систем и сетей. Для определения угроз безопасности информации могут использоваться иные источники, в том числе опубликованные в общедоступных источниках данные об уязвимостях, компьютерных атаках, вредоносном программном обеспечении, а также результаты специально проведенных исследований по выявлению угроз безопасности информации.

Пример определения сценариев реализации угроз безопасности информации приведен на рисунке 11.

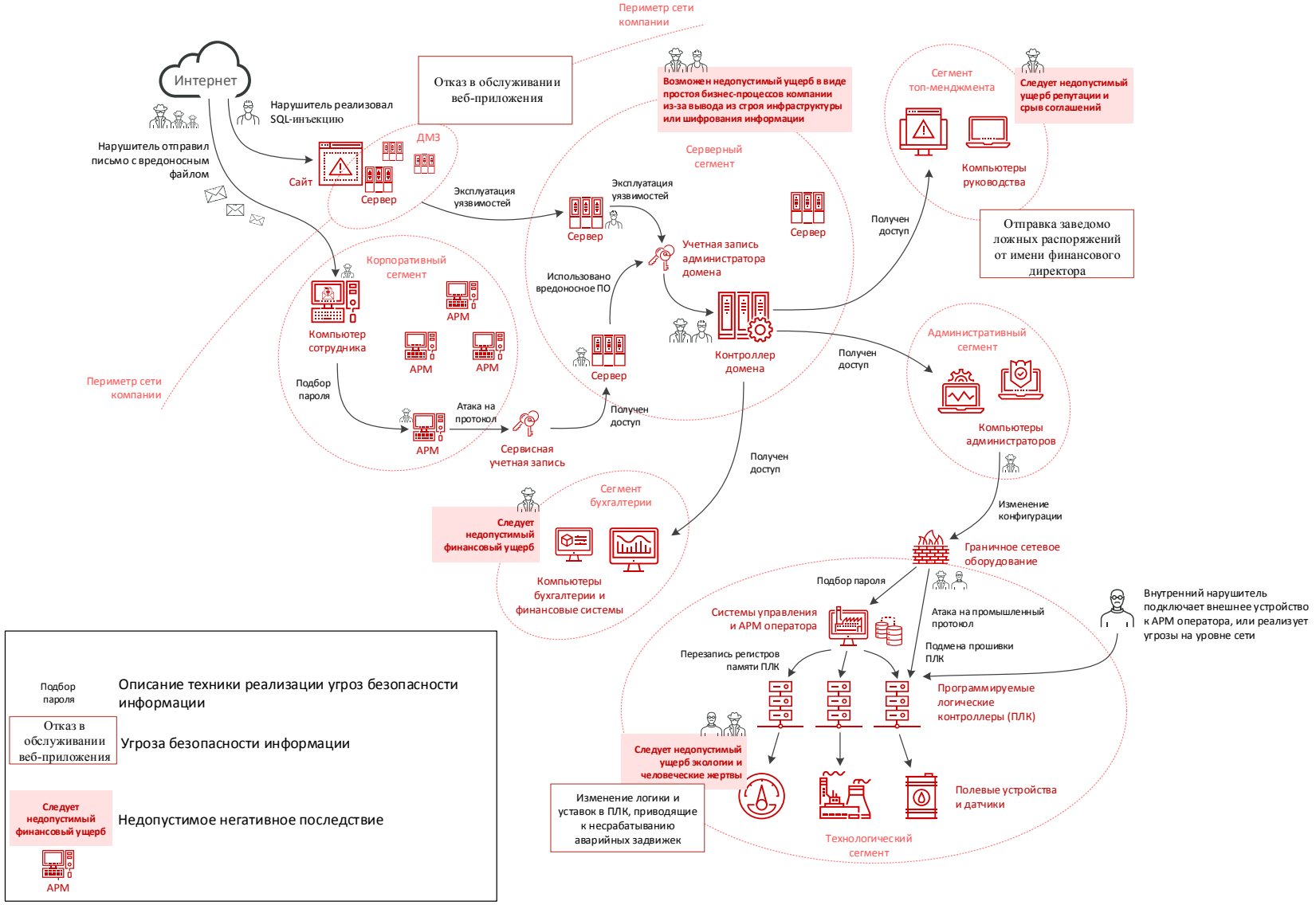

Рисунок 11 - Примеры действий нарушителя, образующих сценарии реализации угроз безопасности информации

7. ОЦЕНКА УРОВНЕЙ ОПАСНОСТИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

7.1. Оценка уровня опасности угроз безопасности информации проводится в отношении каждой i – ой угрозы безопасности информации с j-м сценарием ее реализации ($УБИ_{ij}$). Если для одной угрозы безопасности информации возможна реализация нескольких сценариев ее реализации, оценка уровня опасности данной угрозы проводится для каждого сценария ее реализации.

7.2. Оценка уровня опасности угрозы безопасности информации предусматривает оценку сложности ее реализации для рассматриваемой архитектуры и условий функционирования систем и сетей, а также возможного масштаба негативных последствий (ущерба) в случае успешной реализации этой угрозы.

По уровням опасности угрозы безопасности информации подразделяются на угрозы высокого, среднего, низкого уровня опасности.

7.3. Уровни опасности угроз безопасности информации определяются как в ходе проектирования системы защиты и внедрения мер защиты информации (обеспечения безопасности), так и в ходе эксплуатации систем и сетей.

В ходе проектирования систем и сетей и внедрения мер защиты информации (обеспечения безопасности) уровни опасности угроз безопасности информации оцениваются с целью определения наиболее уязвимых информационных ресурсов и компонентов систем и сетей. В ходе эксплуатации систем и сетей уровни опасности угроз безопасности информации определяются с целью установления приоритетов в реализации мероприятий по защите информации (обеспечению безопасности).

7.4. Уровень опасности угрозы безопасности информации определяется путем оценки следующих показателей:

а) тип доступа к системе или сети, необходимый для реализации сценария угрозы безопасности информации;

б) сложность сценария реализации угрозы безопасности информации;

в) уровень значимости информационных ресурсов или компонентов, на которые направлена угроза безопасности информации.

7.5. По типу доступа к системе или сети угрозы безопасности информации подразделяются на физические, локальные, удаленные (таблица 5).

Таблица 5

Тип доступа	Описание типов доступа
Физический	Сценарий реализации угрозы безопасности информации предусматривает физический доступ нарушителя к средствам обработки и хранения информации. Например, угроза вывода из строя или хищения машинного носителя информации
Локальный	Сценарий реализации угрозы безопасности информации предусматривает локальный доступ (наличие локальной учетной записи) нарушителя к системе или сети. Например, угроза несанкционированного изменения настроек программного обеспечения от имени системного администратора
Удаленный	Сценарий реализации угрозы безопасности информации предусматривает доступ нарушителя к системе или сети, реализуемым посредством сетевого удаленного взаимодействия. Угрозы безопасности информации могут быть удаленно реализуемый, когда реализация угроз происходит на уровне протокола одного или нескольких сетевых переходов (например, через несколько маршрутизаторов), и смежной, когда реализация угрозы происходит из общей физической или логической сети и ограничена только логически смежной топологией. Например, угроза отказа в обслуживании путем отправки специально созданного TCP-пакета

7.6. По сложности сценария реализации угрозы безопасности информации подразделяются на угрозы безопасности информации, имеющие высокий, средний, повышенный и умеренный уровень сложности (таблица 6).

Таблица 6

Уровень сложности	Описание уровней сложности
Умеренный	Сценарий реализации угроз безопасности информации может быть реализован нарушителем с базовым потенциалом
Повышенный	Сценарий реализации угроз безопасности информации может быть реализован нарушителем с базовым повышенным потенциалом

Средний	Сценарий реализации угроз безопасности информации может быть реализован нарушителем со средним потенциалом
Высокий	Сценарий реализации угроз безопасности информации может быть реализован нарушителем с высоким потенциалом

7.7. По уровню значимости информационных ресурсов или компонентов, на которые направлена угроза безопасности информации, угрозы подразделяются на угрозы, направленные на информационные ресурсы или компоненты низкой значимости, угрозы, направленные на информационные ресурсы или компоненты средней значимости, и угрозы, направленные на информационные ресурсы или компоненты высокой значимости (таблица 7).

Таблица 7

Значимость информационных ресурсов и (или) компонентов	**Описание**
Низкая	В результате реализации угрозы будет нарушена безопасность информации, относящейся к одному пользователю, или система (сеть) сможет выполнять возложенные на нее функции (обеспечивать критический процесс) с недостаточной эффективностью или для выполнения функций (обеспечения критического процесса) потребуется привлечение дополнительных сил и средств
Средняя	В результате реализации угрозы безопасности информации будет нарушена безопасность информации, относящейся более чем к одному пользователю, или система (сеть) не сможет выполнять хотя бы одну из возложенных на нее функций или обеспечивать один критический процесс
Высокая	В результате реализации угрозы безопасности информации будет нарушена безопасность информации, относящейся ко всем пользователям, или система (сеть) не сможет выполнять возложенные на нее функции или обеспечивать критические процессы

7.8. Для каждого показателя установлены и приведены в таблице 8 числовые значения, сопоставленные с семантическими значениями таких показателей, описанными в разделах 7.5 – 7.7.

Таблица 8

Показатель уровня опасности	**Значения показателей уровня опасности**	
Тип доступа (*d*)	Удаленный	3
	Локальный	2
	Физический	1
Уровень сложности (*p*)	Умеренный	4
	Повышенный	3
	Средний	2
	Высокий	1
Значимость информационных ресурсов, компонентов (*s*)	Низкая	1
	Средняя	2
	Высокая	3

На основе числовых значений показателей уровня опасности угрозы безопасности информации, определяемых с использованием таблицы 8, рассчитывается их сумма (w):

$$W = d + p + s$$

На основе суммы числовых значений показателей определяется уровень опасности каждой угрозы безопасности информации (w) с j-м сценарием ее реализации в соответствии с таблицей 9.

Таблица 9

Уровень опасности угрозы безопасности информации	**Диапазон значений (*w*)**
Низкий	$w \leq 4$
Средний	$5 \leq w \leq 7$
Высокий	$8 \leq w$

7.10. Угроза безопасности информации подлежит описанию в формате, приведенной в таблице 10.

Таблица 10

Идентификатор	Указывается идентификатор, содержащийся в банке данных угроз безопасности или ином источнике
Наименование	Указывается наименование угрозы, содержащееся в банке данных угроз безопасности
Описание	Указывается описание угрозы, содержащееся в банке данных угроз безопасности или ином источнике
Сценарии	Описываются все возможные сценарии реализации угроз безопасности информации
Уровень опасности	Указывается значение уровня опасности угрозы с конкретным сценарием ее реализации

Приложение № 1 к
Методике моделирования угроз
безопасности информации

Термины и определения, применяемые для целей настоящего методического документа

Архитектура систем и сетей: совокупность основных структурно-функциональных характеристик и свойств систем и сетей, воплощенных в информационных ресурсах и компонентах, правилах их взаимодействия, режимах обработки информации.

Взаимодействующая (смежная) система: система или сеть, которая в рамках установленных функций имеет сетевое взаимодействие с системой или сетью оператора и не включена им в границу моделирования угроз безопасности информации.

Граница моделирования угроз безопасности информации: совокупность информационных ресурсов и компонентов систем и сетей, в пределах которой обеспечивается защита информации в соответствии с едиными правилами и процедурами, а также контроль за реализованными мерами защиты информации.

Информационно-телекоммуникационная (информационная) инфраструктура: совокупность информационных (автоматизированных) систем, информационно-телекоммуникационных сетей, сайтов в сети Интернет, отдельных средств вычислительной техники, программного обеспечения, обеспечивающих систем, используемых оператором для реализации функций (полномочий) или видов деятельности.

Информационные ресурсы: данные, информация, процессы, информационные (автоматизированные) системы, информационно-телекоммуникационные сети, сайты в сети Интернет, входящее в состав системы или сети.

Компонент системы (сети): программное, программно-аппаратное или техническое средство, входящее в состав системы или сети.

Локальный доступ: доступ субъектов доступа к объектам доступа, осуществляемый непосредственно через подключение (доступ) к компоненту систем или через локальную вычислительную сеть (без использования информационно-телекоммуникационной сети).

Обладатель информации: лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Оператор: лицо, осуществляющее деятельность по эксплуатации информационной системы или сети, в том числе по обработке содержащейся в них информации**.**

Пользователь: лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в системе или сети и использующее результаты ее функционирования.

Поставщик услуг: лицо, предоставляющее оператору и (или) обладателю на основании договора или ином законном основании услуги по использованию своих вычислительных ресурсов, программного обеспечения, средств хранения или передачи информации.

Программно-аппаратное средство: устройство, состоящее из аппаратного обеспечения и функционирующего на нем программного обеспечения, участвующее в формировании, обработке, передаче или приеме информации в информационной инфраструктуре.

Удаленный доступ: процесс получения с использованием сетевых протоколов доступа (через внешнюю сеть) к объектам доступа систем и сетей из другой системы и сети или со средством вычислительной техники, не являющимся постоянно (непосредственно) соединенным физически или логически с системой, к которой он получает доступ.

Уязвимость: недостаток (слабость) системы или сети, который (которая) создает потенциальные или реально существующие условия для реализации или проявления угроз безопасности информации.

Приложение № 2 к
Методике моделирования угроз
безопасности информации

Рекомендации по формированию экспертной группы и проведению экспертной оценки при моделировании угроз безопасности информации

Качественное формирование экспертной группы способствует снижению субъективных факторов при моделировании угроз безопасности информации. Занижение (ослабление) экспертами прогнозов и предположений при моделировании угроз может повлечь наступление непрогнозируемого (неожиданного) ущерба в результате их реализации. Завышение экспертами прогнозов и предположений при моделировании угроз безопасности информации может повлечь за собой неоправданные расходы на нейтрализацию (блокирование) угроз, являющихся неактуальными.

Независимо от результата формирования экспертной группы при моделировании угроз безопасности информации существуют субъективные факторы, связанные с психологией принятия решений. Это также может приводить как к занижению (ослаблению), так и к завышению (усилению) экспертами прогнозов и предположений при моделировании угроз безопасности информации, что в свою очередь может привести к пропуску отдельных угроз безопасности информации или к неоправданным затратам на нейтрализацию неактуальных угроз.

Любое решение, принимаемое экспертами при моделировании угроз безопасности информации, должно исходить из правил, при которых нарушитель находится в наилучших условиях для реализации угрозы безопасности (принципа «гарантированности»).

а) формирование экспертной группы

В состав экспертной группы для моделирования угроз безопасности информации рекомендуется включать экспертов (независимо от того, реализуются ли функции обладателя информации, заказчика и оператора в рамках одной или нескольких организаций):

от подразделений обладателей информации, содержащейся в системах и сетях;

от подразделений оператора;

от подразделения по защите информации (обеспечения безопасности);

от лиц, предоставляющих услуги или сервисы;

от разработчиков систем и сетей;

от операторов взаимодействующих систем и сетей.

В качестве экспертов рекомендуется привлекать специалистов, деятельность которых связана с обработкой информации в системах и сетях, а также специалистов, имеющих квалификацию и опыт работы в области применения информационных технологий и в области защиты информации (обеспечения информационной безопасности).

При привлечении в качестве экспертов специалистов от подразделений по защите информации рекомендуется привлекать лиц, имеющих высшее образование или прошедших переподготовку (повышение квалификации) по направлению подготовки «Информационная безопасность», или имеющих не менее трех лет стажа практической работы в своей сфере деятельности.

Эксперты должны обладать независимостью, основанной на отсутствии коммерческого и финансового интереса или другого давления, которое может оказать влияние на принимаемые решения. Не рекомендуется формировать экспертную группу из участников, находящихся в прямом подчинении, так как это может негативным образом повлиять на результат определения угроз безопасности информации.

Состав экспертной группы зависит от назначения систем и сетей, но не должен быть меньше трех экспертов.

б) проведение экспертной оценки

При проведении экспертной оценки принимаются меры, направленные на снижение уровня субъективности и неопределенности при определении каждой из угроз безопасности информации.

Экспертную оценку рекомендуется проводить в отношении, как минимум, следующих параметров:

а) негативные последствия от реализации угроз безопасности информации;

б) цели реализации угроз безопасности информации, категория, виды и возможности нарушителей;

в) условия реализации угроз безопасности информации;

г) сценарии действий нарушителей при реализации угроз безопасности информации;

д) характеристики опасности угроз безопасности информации.

Оценку параметров рекомендуется проводить опросным методом с составлением анкеты, в которой указываются вопросы и возможные варианты

ответа в единой принятой шкале измерений («низкий», «средний», «высокий» или «да», «нет» или иные шкалы). При этом вопросы должны быть четкими и однозначно трактуемыми, предполагать однозначные ответы.

Опрос экспертов включает следующие этапы:

каждый эксперт проводит оценку оцениваемого параметра (рекомендуется не мене двух раундов оценки), результаты которой заносятся в таблицу 1.1;

после оценки каждым из экспертов отбрасываются минимальные и максимальные значения;

определяется среднее значение оцениваемого параметра в каждом раунде;

определяется итоговое среднее значение оцениваемого параметра.

Пример таблицы результатов оценки параметров

Таблица 2.1

Эксперты	Значение оцениваемого параметра (раунд 1)	Значение оцениваемого параметра (раунд 2)
Эксперт 1		
Эксперт 2		
Эксперт n		
Итоговое значение		

Приложение № 3 к
Методике моделирования угроз
безопасности информации

УТВЕРЖДАЮ

Руководитель органа
государственной власти
(организации) или иное
уполномоченное лицо

_____

«___» _____20__г.

Модель угроз безопасности информации

«_____»

наименование системы и (или) сети

1. Общие положения

Раздел «Общие положения» содержит назначение и область действия документа, наименование систем и сети, для которых разработана модель угроз безопасности информации, а также информацию об использованных нормативных правовых актах, методических документах, национальных стандартах, а также источниках, на основе которых определены угрозы безопасности информации.

2. Характеристика информационной инфраструктуры

Раздел «Характеристика информационной инфраструктуры» содержит:

описание информационных ресурсов и компонентов систем и сетей, обрабатывающих, хранящих информацию и (или) обеспечивающих реализацию основных (критических) процессов (бизнес-процессов), категории (роли) пользователей, интерфейсы взаимодействия с пользователями, со смежными (взаимодействующими) системами и сетями, а также состав и типы обеспечивающих систем, включенных в границу моделирования угроз безопасности информации;

назначение систем и сетей (если в границу включены несколько сетей и систем) и основных компонент систем и сетей, выполняемые им функции, решаемые с их использование задачи;

маршруты передачи информации между компонентами систем и сетей;

описание режимов обработки информации;

наличие и способы взаимодействия систем и сетей с сетью Интернет.

В случае если информационные системы и сети функционируют на базе информационно-телекоммуникационной инфраструктуры центра обработки данных, в модель угроз безопасности информации включается описание архитектура этой информационно-телекоммуникационной инфраструктуры.

3. Возможные негативные последствия от реализации угроз безопасности информации

Раздел «Возможные последствия от реализации угроз безопасности информации» содержит описание:

возможных негативных последствий, конкретизированных применительно к областям и особенностям деятельности обладателя информации и (или) оператора;

информационных ресурсов и компонентов систем и сетей, обрабатывающих, хранящих информацию и (или) обеспечивающих реализацию

основных (критических) процессов (бизнес-процессов), неправомерный доступ к которым или воздействие на которые может привести к негативным последствиям;

видов неправомерного доступа и (или) воздействий на информационные ресурсы и компоненты систем и сетей, которые могут привести к наступлению негативных последствий (угрозы безопасности информации).

4. Источники угроз безопасности информации и результаты оценки возможностей нарушителя (модель нарушителя)

Раздел «Источники угроз безопасности информации и результаты оценки возможностей нарушителя (модель нарушителя)» содержит описание:

источников угроз безопасности информации;

возможных целей реализации угроз безопасности информации нарушителями;

категорий и видов нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы (актуальные нарушители);

возможности каждого вида нарушителей по реализации угроз безопасности информации в соответствии с архитектурой и условиями функционирования систем и сетей.

5. Сценарии реализации угроз безопасности информации

Раздел «Сценарии реализации угроз безопасности информации» содержит перечень угроз безопасности информации для рассматриваемых архитектуры и условий систем и сетей. Для каждой угрозы безопасности информации должным быть приведены:

источник угрозы безопасности информации, категория и вид нарушителя;

условия для реализации угроз безопасности информации;

описание сценариев реализации угрозы безопасности информации;

возможные последствия от реализации угрозы безопасности информации.

6. Результаты оценки уровня опасности угроз безопасности информации

Раздел «Результаты оценки уровня опасности потенциальных угроз безопасности информации» содержит уровни опасности каждой угрозы безопасности информации с конкретными сценариями ее реализации.